MATH 347 HW8

Charles Swarts
swarts2@illinois.edu

November 2016

1 Q 1

the official definition of divisibility $a \mid b \coloneqq \exists\, m \in \mathbb{Z} : b = ma$

1.1 a

If $d \mid a$ and $d \mid b$, then $d \mid ax + by$ for any $x, y \in \mathbb{Z}$.

Premise: direct method.

Suppose it is the case that $d \mid a$ and $d \mid b$. And also suppose we are given $x, y \in \mathbb{Z}$
Then by definition of divisibility

$$d \mid a \coloneqq \exists\, m \in \mathbb{Z} : a = md$$

$$d \mid b \coloneqq \exists\, n \in \mathbb{Z} : b = nd$$

Then by the rules of standard algebra

$$ax + by = xmd + ynd$$

$$ax + by = (xm + yn)d$$

By closure (i.e. since the integers are closed under addition and multiplication i.e. an integer plus an integer is an integer, and an integer times an integer is an integer) $(xm + yn) \in \mathbb{Z}$

And again by definition of divisibility,

$$d \mid ax + by$$

■

1.2 b

If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Premise: direct method.

Suppose it is the case that $a \mid b$ and $c \mid d$.

Then by definition of divisibility,

$$a \mid b \coloneqq \exists\, m \in \mathbb{Z} : b = ma$$

$$c \mid d \coloneqq \exists\, n \in \mathbb{Z} : d = nc$$

Then by the rules of standard algebra

$$b \cdot d = ma \cdot nc$$

$$bd = mn \cdot ac$$

By closure $bd, ac, mn \in \mathbb{Z}$

By the definition of divisibility,

$$ac \mid bd$$

$\blacksquare$

1.3 c

If $a \mid b$ and $c \mid d$, then $(a + c) \mid (b + d)$.

Premise: counter-example

Let $a = 1,\ b = 2,\ c = 3,\ d = 3$

By definition of divisibility:

$$a \mid b \coloneqq \exists\, m \in \mathbb{Z} : b = ma$$
$$c \mid d \coloneqq \exists\, n \in \mathbb{Z} : d = nc$$

Since $2 \in \mathbb{Z}$ and $b = 2a$, by definition $a \mid b$. Since $1 \in \mathbb{Z}$ and $d = 1c$, by definition $c \mid d$. However

$$(a + c) = 4 \qquad\qquad (b + d) = 5$$

So if $(a + c) \mid (b + d)$, by definition,

$$\begin{aligned} \exists\, l \in \mathbb{Z} : \qquad (b + d) &= l(a + c) \\ \frac{(b + d)}{a + c} &= l \\ \frac{5}{4} &\in \mathbb{Z} \qquad ※ \end{aligned}$$

Hence we have found an example where $a \mid b$ and $c \mid d$, but $\cancel{(a + c) \mid (b + d)}$ $\blacksquare$

2 Q 2

basic definition of congruence: $a \equiv b \bmod m \coloneqq \exists\, k \in \mathbb{Z} : a = b + km$

2.1 a

If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.

Premise: direct method.

Suppose $a \equiv b \bmod m$ and $c \equiv d \bmod m$.
Then by definition of congruence:

$$\exists\, j \in \mathbb{Z} : a = b + jm$$
$$\exists\, k \in \mathbb{Z} : c = d + km$$

Then by the rules of standard algebra

$$a \cdot c = (b + jm) \cdot (d + km)$$
$$ac = bd + (b \cdot km + jm \cdot d + jm \cdot km)$$
$$ac = bd + m \cdot (bk + jd + jkm)$$

By closure $(bk + jd + jkm) \in \mathbb{Z}$

So by definition of congruence $ac \equiv bd \bmod m$ $\blacksquare$

2.2 b

If $a \equiv b \bmod m$, then for any $k \in \mathbb{N}$, $a^k \equiv b^k \bmod m$.

Premise: induction on i

Base case: Suppose $a \equiv b \bmod m$. Then by the previous proof, using its framework, we let $c = a$ and $d = b$. The result is that $a^2 \equiv b^2 \bmod m$.

Inductive case: Suppose $a^i \equiv b^i \bmod m$. Then by the previous proof, using its framework, we let $c = a$ and $d = b$. The result is that $a^{i+1} \equiv b^{i+1} \bmod m$.

By the principle of induction, if $a \equiv b \bmod m$, then $a^k \equiv b^k \bmod m$. ■

3 3

Let $\mathbb{P}$ represent the set of all prime numbers. *Fermat's Little Theorem:* $p \in \mathbb{P} \Rightarrow a^p \equiv a \bmod p$

3.1 a

Fine the last decimal digit of 347^{101}.

Premise: Since we are using the base 10 number system, finding the congruence mod 10 from the set $\{0\} \cup [9]$ should give the last digit.

Firstly using result from 2.b, we see

$$347 \equiv b \bmod 10 \Rightarrow 347^{101} \equiv b^{101} \bmod 10$$

It is trivial to see that in this base,

$$347 \equiv 7 \bmod 10$$

So now we use the same process, using 2.a and 2.b

$$7^{101} \equiv 7 \cdot 7^{100} \equiv 7 \cdot 49^{50} \equiv 7 \cdot 9^{50} \equiv 7 \cdot 81^{25} \equiv 7 \cdot 1^{25} \equiv 7 \bmod 10$$

So the last digit must be 7.

3.2 b

Find the remainder of 347^{101} when divided by 101.

Premise: to find the remainder, we need to find the number from the set $\{0\} \cup [101]$ that is congruent to $347^{101} \bmod 101$.

Using Fermat's Little Theorem, we see that

$$347^{101} \equiv 347 \bmod 101$$

Which is most of the way, except $347 \notin \{0\} \cup [101]$

Luckily we know the definition of congruence

$$a \equiv b \bmod m := \exists\, k \in \mathbb{Z} : a = b + km$$

So

$$347 \equiv 347 + -3(101) \bmod 101 \equiv 44$$

So the remainder is 44. ■

3.3 c

Using Fermat's Little Theorem, find a number between 0 and 12 that is congruent to 2^{100} modulo 13.

Premise: use Fermat's Little Theorem, 2.a.

Since we know Fermat's theorem, we know

$$2^{13} \equiv 2 \bmod 13$$

Using this fact and 2.a, we can compute

$$2^{100} \equiv 2^9 \cdot 2^{13} \cdot 2^{13} \cdot 2^{13} \cdot 2^{13} \cdot 2^{13} \cdot 2^{13} \cdot 2^{13}$$

$$\equiv 2^9 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \equiv 2^{13} * 2^3 \equiv 2 \cdot 2^3 \equiv 2^4 \equiv 16 \bmod 13$$

Luckily we know the definition of congruence

$$a \equiv b \bmod m \coloneqq \exists\, k \in \mathbb{Z} : a = b + km$$

So

$$16 \equiv 16 + (-1) \cdot 13 \equiv 3 \bmod 13$$

So 3 is the number between 0 1nd 12 that is congruent to 2^{100}. ■

3.4 d

Find the last digit in the base 8 expansion of (i)9^{1000},(ii)10^{1000},(iii)11^{1000}.

Premise: Since we are converting to octal, we need to find the number which is congruent mod 8 and in the the set $\{0\} \cup [7]$.

3.4.1 i

By the definition of congruence

$$9 \equiv 9 + (-1)8 \equiv 1 \bmod 8$$

Since we know that, by 2.b

$$9^{1000} \equiv 1^{1000} \equiv 1 \bmod 8$$

So the last digit in octal will be 1.

3.4.2 ii

By the definition of congruence

$$10 \equiv 10 + (-1)8 \equiv 2 \bmod 8$$

Since we know that, by 2.b

$$10^{1000} \equiv 2^{1000} \equiv 8^{250} \bmod 8$$

By definition of congruence

$$8 \equiv 8 + (-1)8 \equiv 0$$

Since we know that, by 2.b

$$8^{250} \equiv 0^{250} = 0 \bmod 8$$

So the last digit in octal will be 0.

3.4.3 iii

By the definition of congruence

$$11 \equiv 11 + (-1)8 \equiv 3 \bmod 8$$

Since we know that, by 2.b

$$11^{1000} \equiv 3^{1000} \equiv 9^{500} \bmod 8$$

By the definition of congruence

$$9 \equiv 9 + (-1)8 \equiv 1 \bmod 8$$

Since we know that, by 2.b

$$9^{500} \equiv 1^{500} = 1 \bmod 8$$

So the last digit in cotal will be 1.